Informática criminalística: una especialidad en desarrollo[*]

Recibido: 12 de abril de 2019 • Aprobado: 30 de mayo de 2019
https://doi.org/10.22395/ojum.v19n38a12

Vladimir Naranjo Gómez[**]
Juan Carlos Mendoza Pérez[***]
Elvys de la Caridad Alonso Betancourt[****]
Jeanders Silvio Hinojosa Calzada[*****]

RESUMEN

Los avances obtenidos en las nuevas tecnologías de la información y las comunicaciones han cambiado las metodologías para aplicar las especialidades tradicionales que conforman la técnica criminalística, además de que han proporcionado el surgimiento de otras en el enfrentamiento a la actividad delictiva[1]. Este trabajo actualiza y se acerca más a la aplicación de la especialidad de referencia, partiendo de la experiencia de su empleo en la provincia de Guantánamo. Se utilizaron varias técnicas de la investigación científica como la entrevista a profundidad, el análisis de documentos, el análisis secundario y el estudio de casos.

Palabras clave: informática criminalística; especialidad; tecnologías de la información; técnica criminalística.

[*] Este artículo es resultado de la actividad investigativa de sus autores que corresponde a la línea de investigación del Departamento de Derecho de la Universidad de Guantánamo, referida al Derecho Informático y a la Sociedad cubana de Derecho e Informática de la Unión de Juristas de Cuba en Guantánamo.

[**] Licenciado en Derecho, magíster en Dirección. Profesor asistente de Criminología y Criminalística, Departamento de Derecho, Universidad de Guantánamo, Guantánamo, Cuba. Correo electrónico: vladimirng@cug.co.cu. Orcid: https://orcid.org/0000-0002-8315-2872

[***] Licenciado en Derecho y estudiante de la Maestría en Derecho Constitucional y Administrativo. Profesor auxiliar de Derecho notarial, Derecho civil, Derecho de obligaciones, Departamento de Derecho, Universidad de Guantánamo, Guantánamo, Cuba. Correos electrónicos: jcperez@cug.co.cu, juan.mendoza@uo.edu.cu. Orcid: https://orcid.org/0000-0003-3197-9605.

[****] Licenciada en Educación. Profesora auxiliar de Inglés, Comunicación social y rural, magíster en Ciencias de la Educación, Universidad de Guantánamo, Guantánamo, Cuba. Correo electrónico: elvys@cug.co.cu. Orcid: https://orcid.org/0000-0002-2838-5737

[*****] Ingeniero informático, licenciado en Derecho y magíster en Ciencias de la Educación. Profesor instructor de Derecho informático de tiempo parcial, Universidad de Guantánamo, Guantánamo, Cuba. jeander@nauta.cu. Orcid: https://orcid.org/0000-0001-7901-875

[1] Cada día es más frecuente la necesidad de la recolección de huellas y evidencias en soportes digitales para enfrentar los más diversos delitos; y en consideración a ellos se hace un mayor empleo de la informática criminalística, especialidad de más reciente creación en la aplicación de los adelantos científico-técnicos en la investigación criminal.

Criminalistic Computer Science: a Developing Specialty

ABSTRACT

The advancements obtained thanks to new technologies of information and communications have changed the methodologies for applying the traditional specialties that conform to the criminalistic technique, alongside the fact that they have helped to the surging of other techniques for confronting criminal activities. This piece of work updates and gets closer to the reference specialty, starting from the experience of its application in the Guantanamo province. Several scientific research techniques were used as In-depth interviewing, document analysis, secondary analysis, and case study.

Keywords: criminalistic computer science; specialty; Information technologies; criminalistic techniques.

Informática criminalística: uma especialidade em desenvolvimento

RESUMO

Os avanços obtidos nas novas tecnologias da informação e da comunicação vêm mudando as metodologias para aplicar as especialidades tradicionais que conformam a técnica criminalística, além de proporcionar o surgimento de outras para enfrentar a atividade criminal. Este trabalho atualiza e se aproxima da aplicação da especialidade de referência ao partir da experiência de sua utilização na província de Guantánamo, Cuba. Foram utilizadas várias técnicas da pesquisa científica como a entrevista a profundidade, a análise documental, a análise secundária e o estudo de casos.

Palavras-chave: informática criminalística; especialidade; tecnologias da informação; técnica criminalística.

INTRODUCCIÓN

La revolución de las tecnologías de la información y la comunicación ha propiciado cambios sustancialmente favorables para la humanidad. Las conexiones digitales reducen significativamente las distancias, incrementan considerablemente los intercambios entre las personas, favorecen el comercio y el acceso a los servicios de todo tipo e impregnan cambios de paradigmas para las personas jurídicas y naturales.

Apoyado en esa nueva realidad, el Estado promueve la sociedad de la información y la aplicación de las nuevas tecnologías a la administración y al pueblo en general que contribuyan al desarrollo integral de la sociedad. En tal sentido fue aprobada la Política de Informatización de la Sociedad Cubana. De ahí los avances de la era digital propiciaron, además del incremento de las actividades delictivas mediante el empleo de los medios tecnológicos de la información y las comunicaciones, bien sea por la comisión de delitos propiamente conceptualizados como informáticos (a pesar de que la legislación penal no tipifica este tipo de conducta), así como de otros delitos.

Hoy, muchas de las huellas y evidencias —cuya recolección es necesaria para demostrar la comisión de un determinado delito— están en soporte digital, por lo que la informática ha permeado casi todos los entornos: la mayoría de los documentos, fotos, videos y controles de recursos de todo tipo se han adaptado al ámbito tecnológico contemporáneo. Así, ha sido necesario perfeccionar las metodologías que garanticen una efectiva búsqueda de los rastros del recorrido que han tomado estos.

Ante esta realidad, surge la informática criminalística como parte de las especialidades que integran la técnica, que hasta la fecha es la de más reciente creación y que tiene sus orígenes en el año 2001. El trabajo actualiza y acerca más a la aplicación de la especialidad de la informática criminalística, partiendo de la experiencia de su empleo en la provincia de Guantánamo. Se utilizaron varias técnicas de la investigación científica como la entrevista a profundidad, el análisis de documentos, el análisis secundario y el estudio de casos. Mostrar el desarrollo que ha tenido la aplicación de la especialidad de la informática criminalística, y su importancia en la investigación del delito, guía el desarrollo de este trabajo.

Es importante asumir que "[a] modo de anotación esencial, partimos de la concepción acerca de que la finalidad del proceso penal no puede ser otra que la materialización de la justicia" (Castaño, 2010, p. 178). En este sentido, el peritaje informático juega un papel relevante en la era moderna.

1. UNA APROXIMACIÓN CONCEPTUAL

La criminalística establece las metodologías que garantizan el empleo del resto de las ciencias en el esclarecimiento de los hechos delictivos. En tal sentido es notable

la forma en que hoy los adelantos de la informática contribuyen al enfrentamiento de la actividad delictiva, ya sea de forma directa o mediante su apoyo al resto de las ciencias que son aplicables a la investigación del hecho criminal.

Dentro de los conceptos de la especialidad de Informática criminalística se define que se encarga de "realizar el estudio criminalístico de las evidencias de carácter informático con el objetivo de aportar elementos para el esclarecimiento de los hechos delictivos" (Colectivo de autores, 2004, p. 44). Esta definición no considera que no solo se trata de la búsqueda de evidencias, sino también de huellas, bajo el principio de que evidencias y huellas no son sinónimos en el orden teórico. Se trata de una definición sencilla, pero que ayuda a comprender el objetivo central que se persigue con el empleo de esta especialidad.

Otras definiciones son más precisas o amplias, como la que plantea que la informática criminalística:

> Es la especialidad encargada de adquisición, análisis, preservación y presentación de la información que ha pasado por un proceso informático, la cual puede haber permanecido almacenada en medios electrónicos relacionados directa o indirectamente con la comisión de hechos delictivos, que pude ser causada por el aumento del valor de la información, así como por su uso, a la creación de nuevas plataformas de empleo de la informática, y las nuevas tecnologías de la información y las comunicaciones. (Colectivo de autores, 2015, p. 70)

En el concepto anterior se amplía la misión que tiene a cargo la especialidad en análisis, apoyada en consideración de que la recolección de las huellas y evidencias considera la existencia de cinco fases, a saber: la búsqueda, revelación, fijación, extracción y conservación[1]. Otros autores se refieren a una fase denominada procesamiento, pero en opinión de los autores de este trabajo no se trata de una sexta fase debido a que la recolección concluye cuando se logran preservar debidamente la huellas y evidencias, y el procesamiento rebasa el proceso de recolección. Es importante considerar en esta definición que las informaciones solamente pueden haber estado en medios electrónicos.

Las fases de la recolección de las huellas y evidencias en materia de peritaje informático se expresa de manera general en la siguiente consideración:

[1] Búsqueda: consiste en la observación que se realiza en el lugar del hecho con el objetivo de localizar las huellas y evidencias. Revelación: consiste en hacer visibles las huellas que no se observan a simple vista, utilizándose para ello métodos físicos y químicos. Fijación: mediante la misma se deja constancia gráfica de las huellas y evidencias, a través de actas, planos, croquis, fotografías del lugar. Extracción: utilizando diferentes medios técnicos se extraen las huellas y evidencias del lugar del hecho. Conservación: fase de recolección de las huellas y evidencias mediante la cual se embalan las pruebas materiales para que no se deterioren y puedan ser objeto de estudio e investigación posterior.

> Para la realización del peritaje de la evidencia digital se emplean técnicas de informática forense, las cuales son un conjunto de métodos destinados a adquirir, preservar y presentar la información valiosa extraída de los distintos dispositivos que manejan memoria informática, sin alterar el estado de los mismos. (Lasso, 2017, p. 23)

Por otro lado, en este análisis hay que considerar la definición que establece que "[l]as evidencias informáticas son los productos de las Nuevas Tecnologías de la Información y las Comunicaciones (NTIC) capaces de producir o soportar datos que permitan contribuir a la demostración científica de la actividad delictiva que fue cometida" (Colectivo de autores, 2007, p. 44). Se plantea con toda claridad que las evidencias informáticas pueden ser producidas o soportadas por los diferentes medios de la nuevas tecnologías, por lo que la investigación debe estar dirigida tanto a la búsqueda de los medios que pueden haber producido, como aquellos que pueden contenerlas.

Para ampliar el debate se puede decir que la informática criminalística es "un proceso metodológico para la recogida y análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales" (Rodríguez *et al*., 2011). En este caso se abordan definiciones expuestas por autores de otros países para que los estudiantes y profesionales puedan contar con otras variantes sobre el tema, a pesar de que existen puntos de coincidencia como la recogida y análisis de los datos digitales.

Roatta *et al*. (2014), al referirse a la informática criminalística, precisan que "[e]l análisis digital forense es la aplicación de técnicas científicas y analíticas especializadas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal" (p. 2). Se aprecia en esta definición la marcada referencia a las fases de recolección de las huellas y evidencias, aspecto que constituye un referente en todos los conceptos relacionados.

2. LA ESPECIALIDAD DE INFORMÁTICA CRIMINALÍSTICA. APUNTES TEÓRICOS-PRÁCTICOS

Algunos libros ubican el nacimiento de la especialidad de informática criminalística en Cuba en el año 2001, pero otros precisan que en 1995 comenzaron a conocerse los primeros hechos delictivos cometidos mediante el empleo de sistemas automatizados. Este hecho obligó al desarrollo de una nueva especialidad que se encargara del estudio de las tecnologías de las información y las comunicaciones con fines criminalísticos. En el año 1999 surgió, entonces, la especialidad de referencia, la cual está integrada por cuatro subdisciplinas que difieren ligeramente en los métodos, procedimientos y propósitos, pero comparten la naturaleza digital del tipo de evidencia y huella que examinan:

1. Video digital
2. Audio digital

3. Imagen digital
4. Informática forense

En ese sentido, en marzo de 1998, la International Organization on Computer Evidence (IOCE) fue designada para trazar principios internacionales en los procedimientos relativos a la evidencia digital y garantizar la armonización de métodos y prácticas entre países.

Principios de la Informática Forense internacionalmente aceptados:

1. Cuando se trata de recolectar evidencia digital, todos los principios y procedimientos generales de la criminalística deberán ser aplicados.
2. Si se ocupa evidencia digital, ninguna acción realizada podrá cambiar la evidencia.
3. Cuando sea necesario que una persona acceda a la evidencia original, deberá ser un profesional forense.
4. Toda actividad relacionada con la ocupación, acceso, almacenamiento o transferencia de evidencia digital debe ser totalmente documentada, preservada y disponible para su revisión.
5. Se establece la responsabilidad individual de todas las acciones realizadas mientras la evidencia digital esté en posesión del individuo.
6. Cualquier agencia que ocupe, acceda, almacene o transfiera evidencia digital es responsable del cumplimiento de estos principios.

Dentro de las reglas generales que se reconocen se encuentran las siguientes:

- Manipulación/contaminación mínima del original.
- Registro detallado de las acciones y cualquier cambio producido.
- Cumplimiento de las cinco reglas de la evidencia.
- No exceder los conocimientos.
- Seguimiento de las políticas locales de seguridad y obtención de los permisos necesarios para acceder a la evidencia.
- Preparación del testimonio.
- Captura de una imagen lo más precisa posible del sistema investigado.
- Aseguramiento de la reproducibilidad de las acciones.
- Trabajo rápido.
- Trabajo con la información volátil y persistente.

- No ejecutar ningún programa en el sistema investigado.
- Documente, documente y documente.

Poco se ha escrito, en la literatura que hoy está disponible para nuestros estudiantes, sobre los diferentes peritajes que ofrece la informática criminalística. Consideramos que es el momento para ilustrar las posibilidades que ofrece esta especialidad en la búsqueda, revelación, fijación, extracción, conservación y procesamiento de las evidencias y huellas digitales.

3. PERITAJES QUE SE REALIZAN POR LA ESPECIALIDAD DE INFORMÁTICA CRIMINALÍSTICA

Estado técnico y aptitud para el uso: verifica la condición de factibilidad del equipo o dispositivo investigado para su rol como evidencia, sea medio (instrumento idóneo), fin (objeto del delito) o soporte de indicios (información vinculada al hecho), al establecer mediante comprobaciones tecnológicas la funcionalidad parcial o total del mismo.

> Cuestiones que resuelve: descarta o señala un equipo o dispositivo investigado dependiendo de las limitaciones funcionales que resulten del peritaje.

Identificación y examen de dispositivos: establece las funciones que realiza un dispositivo investigado desconocido y extrae información del sistema de memoria.

> Cuestiones que resuelve: determina la participación de un dispositivo como instrumento idóneo para la consumación del hecho que se investiga y aporta datos de configuración o bitácoras de procesos que constituyen medio de prueba de la actividad delictiva que se investiga.

Revelación de datos: pesquisa orientada que se practica sobre el área de datos persistentes en estado vigente e incluye los enmascarados e ilegibles, con el propósito de aportar información que pruebe un hecho delictivo vinculado al elemento peritado.

> Cuestiones que resuelve: localiza, describe e ilustra de forma tangible ficheros vigentes y sus contenidos de valor probatorio para documentarlos como medio de prueba.

Recuperación de datos: pesquisa orientada que se practica sobre el área no asignada a datos y el espacio residual de ficheros y particiones con el propósito de recuperar parcial o totalmente los datos persistentes en estado eliminado para aportar información o fragmentos que prueben un hecho delictivo vinculado al elemento peritado. Incluye los elementos enmascarados e ilegibles que a pesar de estar eliminados no se encuentran sobrescritos.

Cuestiones que resuelve: localiza, describe e ilustra de forma tangible ficheros eliminados y sus contenidos de valor probatorio para documentarlos como medio de prueba.

Cotejo y descarte de ficheros: comparación cualitativa y cuantitativa de ficheros a partir de sus valores hash, registros descriptivos, metadatos y MAC o datas de modificación / acceso /creación.

Cuestiones que resuelve: determina la legitimidad de un fichero, discrimina si es una copia y diagnostica las formas de diseminación del mismo. Descarta o selecciona grandes volúmenes de datos a partir registros NSRL conocidos.

Peritaje Integral: pesquisa no orientada que se practica sobre todo el espacio físico del dispositivo evidencia con el propósito de revelar, recuperar, comparar y analizar datos persistentes con independencia de su estado para aportar información o fragmentos que prueben un hecho delictivo vinculado al elemento peritado.

Cuestiones que resuelve: localiza, describe e ilustra de forma tangible ficheros y sus contenidos de valor probatorio para documentarlos como medio de prueba.

Peritaje de orientación: aporta Información panorámica de los datos almacenados en un dispositivo (resumen de toda la información), basados en los datos de tipo multimedia (fotografía digital, audio/video), configuraciones y servicios internet (presencia), uso de acceso telefónico a redes y mensajería electrónica.

Cuestiones que resuelve: se cuantifica la información obtenida y se le da la posibilidad de la copia digital de la información. El órgano solicitante debe remitir el soporte para guardarla.

Réplica digital, certificación y ampliación: partiendo de la evidencia original, se hace una réplica física para que otros especialistas designados por el órgano solicitante practiquen las pesquisas.

Cuestiones que resuelve: si el resultado de la pesquisa es positivo, se certifica y se amplía si fuera necesario. Si el resultado es negativo y el órgano solicitante está interesado en peritar esas evidencias, se practica la pesquisa a la réplica por parte de la sección de informática. Se debe remitir un soporte para el trasiego con la réplica del dispositivo investigado.

Arqueología digital: orientada a obtener información de los usuarios (personas o instituciones) de un dispositivo para establecer el origen del mismo.

Cuestiones que resuelve: dependiendo del tipo de información obtenida, los datos pueden ser utilizados como elementos identificatorios, por lo que su utilidad está relacionada con el hecho que se investiga.

Geología digital: estudia los procesos asociados a los dispositivos que conforman la arquitectura de la computadora y los que se agregan como resultado de las necesidades de los usuarios.

Cuestiones que resuelve: brinda a la investigación elementos que permiten establecer el tiempo, un evento asociado con un propósito particular, un proceso que se haya hecho y que resulte de interés para la investigación.

Investigaciones especiales

Término de los peritajes

1. Treinta días (baja complejidad)
   a. Se dispone de muestras o referencias de procedencia debidamente conocida.
   b. El volumen nominal total de datos es de hasta 40 GB en discos fijos, 5 GB en soportes de almacenamiento masivo y hasta 20 unidades de menos de 100 MB[2].
   c. No contiene evidencias con dispositivos especiales[3].
   d. No se requiere de análisis especiales: criptoanálisis o estegoanálisis[4].

[2] Un disco duro es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales. El disco fijo está unido al dispositivo que lo sostiene. Tiene que estar atornillado al equipo, lo cual impide su movimiento. El soporte de almacenamiento de datos o medio de almacenamiento de datos es el material físico donde se almacenan los datos que pueden ser procesados por una computadora, un dispositivo electrónico y un sistema informático. Los soportes de almacenamiento masivo se refieren al almacenamiento de gran volumen de información digitalizada. Un *gigabyte* es una unidad de almacenamiento de información cuyo símbolo es GB, equivalente a 109 (1 000 000 000 -mil millones-) de bytes. B*yte* es la unidad de información de base utilizada en computación y en telecomunicaciones. El *megabyte* (MB) es una unidad de información. Coloquialmente a los megabytes se les denomina *megas*.

[3] Los dispositivos especiales son cualquier dispositivo, software, equipo, sistema o instrumento fabricado, desarrollado o adaptado que permita superar y/o eliminar las barreras arquitectónicas. Son los que se utilizan para sistemas de seguridad en instalaciones públicas o privadas, los empleados en el diagnóstico y tratamiento de enfermedades.

[4] El criptoanálisis se ocupa de conseguir capturar el significado de mensajes construidos mediante criptografía sin tener autorización para ello. La criptografía se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones de las personas y entidades que se comunican. El estegoanálisis se ocupa de detectar mensajes ocultos con técnicas esteganográficas. Podríamos decir que el estegoanálisis tiene un objetivo opuesto al de la esteganografía. La esteganografía se ocupa de ocultar mensajes con información privada por un canal inseguro, de forma que el mensaje no sea ni siquiera percibido. Normalmente el mensaje es escondido dentro de datos con formatos de video, imágenes, audio o mensajes de texto.

II. Sesenta días (mediana complejidad)

a. Se dispone de muestras o referencias indubitadas.

b. El volumen nominal total de datos es entre 40 y 80 GB en discos fijos, 5 GB en soportes de almacenamiento masivo y 20 unidades de menos de 100 MB.

c. Contiene evidencias con dispositivos especiales, de los cuales se cuenta con los medios idóneos para su adquisición.

d. No requiere de análisis especiales: criptoanálisis o estegoanálisis.

e. Requiere de estudios complementarios.

III. Noventa días (alta complejidad)

a. El volumen nominal total de datos supera los 80 GB en discos fijos.

b. No se dispone de muestras o referencias indubitadas.

c. Contiene evidencias con dispositivos especiales, de los cuales no se cuenta con medios idóneos para su adquisición.

d. Requiere de análisis especiales: criptoanálisis o estegoanálisis.

e. Requiere de estudios complementarios.

4. APLICACIÓN DE LA ESPECIALIDAD DE LA INFORMÁTICA CRIMINALÍSTICA EN LA PROVINCIA DE GUANTÁNAMO

Para esta investigación fue seleccionada una muestra correspondiente a los años del 2015 al 2018. El análisis que se realizó sobre los datos obtenidos del peritaje informático efectuado a varias Tecnologías de Información y las Comunicaciones (TIC) involucrados en la comisión de hechos delictivos revela un incremento de estos en el territorio guantanamero. Al cierre del mes de octubre del año 2018 se registraban un total de cuarenta peritajes, en los cuales fue preciso aplicar la informática criminalística, doce más que en igual periodo del año anterior. Se mantuvo una tendencia al incremento al analizar el comportamiento de estos desde el año 2015 hasta el 2019.

Igual situación se observa con respecto a la utilización de las TIC para la comisión de hechos delictivos previstos en el título "Delitos contra el normal desarrollo de las relaciones sexuales, y contra la familia, la infancia y la juventud" del código penal cubano. En tal sentido se aprecia una especial utilización de las TIC para la comisión de hechos de ultraje sexual, previstos en el artículo 303 del código penal cubano, fundamentalmente vinculados al inciso c, el cual se refleja en el 3,9 % de los delitos

computados. De igual forma se emplean dichos medios en los actos de violación, los abusos lascivos y la corrupción de menores. No obstante, independientemente de su poca presencia, la utilización del internet para la difusión de los materiales fílmicos realizados durante la consumación de las tipologías de delitos señaladas con anterioridad, incrementan exponencialmente el impacto social de estas conductas.

Resalta la utilización de las TIC en delitos en los cuales su presencia no era común en años anteriores. Esto está en consonancia con la actualización de los *modus operandi* y la facilidad de los autores para acceder a un medio informático. Tal es el caso de los delitos de atentado y evasión fiscal, previstos en los artículos 142.1 y 343.1, 2, 3 respectivamente, del Código Penal Cubano.

Se mantiene la tendencia al incremento de los delitos vinculados al patrimonio y la economía nacional, lo que afecta fundamentalmente al sector estatal. Resaltan entre ellos los delitos de malversación, hurto y robo con fuerza, los que en su conjunto suman un total de veinte hechos, los cuales representan el 25,6 % de la muestra seleccionada. No obstante, desataca la ocurrencia de nueve hechos de cohecho, en su mayoría vinculados a delitos del mismo carácter.

5. CAMBIOS DE PARADIGMAS

El desarrollo de la informática, que incluye la digitalización de todo tipo de imagen, convoca a la reflexión sobre la necesidad de que perdure como especialidad independiente la fotografía y videos. De ahí que los medios convencionales para realizar fotografía y videos han quedado atrás. Hoy todo transita por la vía digital desde el uso de un sencillo celular hasta la más sofisticada cámara tecnológica digital, que alcanzan un nivel de precisión que hace apenas unos años parecía obra de la ciencia ficción.

Como parte de esta investigación, los especialistas entrevistados no recordaban el caso más reciente en que haya sido necesario acudir al empleo de la especialidad de fotografía y videos en la búsqueda de huellas y evidencias para el esclarecimiento de un hecho presuntamente delictivo. Máxime si acreditamos que cada día son más frecuentes los casos en que resulta necesaria la utilización de los procedimientos de la especialidad de la informática criminalística para el procesamiento de fotos y videos contenidos en diferentes soportes digitales, que han estado vinculados a la comisión de un supuesto hecho delictivo.

Al valorar cómo transciende en la actualidad el avance de la ciencia en la investigación del delito, el investigador cubano Brito Flebes (2001) resalta el impacto que hoy tiene el desarrollo de la computación en el procesamiento de imágenes y en la identificación de personas por sus rasgos exteriores, al señalar que:

> La computación permite el procesamiento de imágenes fotográficas favoreciendo que determinados objetos que aparecen imprecisos, oscuros, duplicados, dobles, corridos, movidos se perfeccionen con vistas a dar una mejor definición de los mismos con una mayor precisión. En la Identificación de personas para la realización del llamado retrato hablado se aplican programas de computación para su confección a partir de las declaraciones de testigos o de la propia víctima. (p. 33)

Ante el impetuoso avance la informática criminalística, ¿qué queda de la especialidad de fotografía y videos en la criminalística cubana? Quizás no queda nada. La mayoría de las fotografías y videos que en la actualidad se obtienen están en soporte digital, con el empleo de medios de la información y las comunicaciones. La informática criminalística responde hoy con eficiencia ante el empleo de las tecnologías en la comisión de los hechos delictivos. El desarrollo tecnológico impone, en este caso, la fusión de ambas especialidades.

Las entrevistas y el análisis de documentos nos guiaron, además, a la conclusión de que el empleo de las técnicas de la informática ha favorecido una mayor eficiencia en el uso de la especialidad de la técnica criminalística denominada Identificación de Personas por sus Rasgos Exteriores (IPRE). El uso de los más avanzados *software* agiliza el empleo de esta especialidad, y garantiza una mayor efectividad de la misma. Ya en ella no juega un papel determinante la habilidad para dibujos del especialista, sino sus conocimientos en el empleo de los medios informáticos.

Se está en el momento histórico de considerar si las especialidades de fotografía y videos e Identificación de Personas por sus Rasgos Exteriores tienen vida propia o forman parte de la informática criminalística. La ciencia informática determina significativamente el cumplimiento de los objetivos de las dos anteriores para no admitir que forman parte de esta última, y deberían estructurarse como peritajes específicos de la especialidad de informática criminalística.

CONCLUSIONES

Se aprecia un amplio empleo de la especialidad de la informática criminalística en investigación de los más variados hechos delictivos. El empleo de las nuevas tecnologías de la información y las comunicaciones en la consumación del delito, que ha significado la ruptura del uso de los convencionales *modus operandi*, trajo aparejado el surgimiento y consolidación de una nueva especialidad de la técnica y la informática criminalística.

La aparición, en mayor frecuencia, de huellas y evidencias de la posible comisión de un hecho delictivo, en los más diversos medios de soporte o transmisión digital, impone nuevos retos a esta joven especialidad para contribuir al esclarecimiento completo, multilateral y objetivo del delito.

Esos nuevos retos incluyen el crecimiento del empleo de la informática y en el desarrollo de las demás especialidades de la técnica criminalística.

Finalmente, se consideran las siguientes recomendaciones a grandes rasgos:

1. Proponer la convivencia de fusionar las especialidades de fotografía y videos e Identificación de Personas por sus Rasgos Exteriores con la especialidad de informática criminalística.

2. Utilizar este material como fondo bibliográfico de la asignatura de criminalística, que se imparte en la carrera de Derecho.

3. Continuar realizando investigaciones sobre el empleo de la informática criminalística en la investigación criminal.

REFERENCIAS

Brito Febles, O. (2001). L*a técnica criminalística*. Universidad de La Habana.

Colectivo de autores. (2015). C*riminalística*. Editorial Universitaria Félix Varela.

Colectivo de autores. (2004). T*emas de criminalística*. Editorial Universitaria Félix Varela.

Colectivo de autores. (2007). T*emas de criminalística*. Editorial Universitaria Félix Varela.

Rodríguez, F. y Doménech, A. (2011). L*a informática forense*: *el rastro digital del crimen*. https://www.derechoycambiosocial.com/revista025/informatica_forense.pdf.

Roatta, S., Casco, M. y Fogliato, M. (2014). E*l tratamiento de la evidencia digital y las normas* ISO/IEC 27037:2012.2014. http://sedici.unlp.edu.ar/bitstream/handle/10915/50586/Documento_completo.pdf-PDFA.pdf.

Lasso, V. (2017). E*stado del peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia*. https://repository.unad.edu.co/handle/10596/17473.